UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/591,545	08/16/2007	Roberto Avanzi	DE04 0062 US1	4844

65913 7590 12/30/2010

NXP, B.V.
NXP INTELLECTUAL PROPERTY & LICENSING
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
HUGHES, KEVIN G	

ART UNIT	PAPER NUMBER
2193	

NOTIFICATION DATE	DELIVERY MODE
12/30/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Office Action Summary	Application No.	Applicant(s)	
	10/591,545	AVANZI, ROBERTO	
	Examiner	Art Unit	
	KEVIN HUGHES	2193	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 September 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/1/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

Claims 1-10 objected to because of the following informalities: Recitations from the claims often fall in prentices but it appears what is cited is intended to be claimed (Ex, claim 1, equations for multi-exponentiation and multi-scalar multiplication). Generally, prentices are reserved for citing Figure elements to further clarify the claim language and no patentable weight is given to the contents of the prentices [See MPEP § 608.01(m)].

Claims 1, 8 and 9 objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim 10. See MPEP § 608.01(n). Accordingly, the claim has not been further treated on the merits. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-10 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 1, it is unclear if the applicant is claiming a method for multi-exponentiation or multi-scalar multiplication or exponentiation or scalar multiplication. For purposes of examination, the multi-exponentiation case will be rejected. Regarding claim 1, the phrase "for example" renders the claim indefinite

because it is unclear whether the limitation(s) following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

Claims are replete with "(multi-)", for purposes of examination it is construed that the multi is a claimed limitation.

Claims are replete with and/or statements, for purposes of examination it is construed as a non-inclusive or statement.

Claims 7-10 provides for the use of a method in hardware, but, since the claim does not set forth any steps involved in the method/process, it is unclear what method/process applicant is intending to encompass. A claim is indefinite where it merely recites a use without any active, positive steps delimiting how this use is actually practiced.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-6 and 10 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1-6 recite a method for performing multi-exponentiation featuring steps for performing recursive mathematical operations without any recitation of hardware elements or a transformation of an article representing a tangible and physical object. The method steps for performing the equations preempt any and all uses of the equations. Therefore the method steps that are central to the process do not explicitly require physical hardware, thus the claimed

method does not define any structural or functional interrelationships between the method and an otherwise statutory class. Additionally, while the steps of computing and finally storing by a processor (steps a and b) require a machine, the required machine does not pose a meaningful limit on the claim's scope because the steps are not central to the purpose of the method invented by applicant, and can be considered merely an extra-solution activity.

Claim 10 recites systems for performing the method of claim 1 but the recited systems are software per se.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-6 rejected under 35 U.S.C. 102(b) as being anticipated by "Improved Techniques for Fast Exponentiation" by Bodo Moller (hereinafter Moller).

As per claim 1, Moller discloses a method for the multi-exponentiation or the multi-scalar multiplication of elements by means of in each case at least one exponent or scalar, in particular an integer exponent or scalar (Introduction [Page 1] paragraph 1 and Multi-Exponent by Interleaved Exponentiation paragraphs 1-2, multi exponentiation is being performed), which has in each case a maximum bit rate or bit length, in

particular for the exponentiation or scalar multiplication of an element by means of at least one exponent or scalar, in particular an integer exponent or scalar, which has in each case a maximum bit rate or bit length, which elements derive from at least one group, for example an Abelian group, which in the case of exponentiation is notated in particular multiplicatively and in the case of scalar multiplication is notated in particular additively (Introduction [Page 1] paragraphs 1-2 and Multi-Exponent by Interleaved Exponentiation paragraphs 1-2, exponentiation of more than one scalar is applied where there are domain parameters for the group to be exponentiated), characterized by the following method steps:[a. 1] computing and storing or[a.2] retrieving from at least one memory all powers or all multiples, wherein c is a permissible positive coefficient (Introduction [Page 1] paragraphs 3-5, a vector of exponents is retrieved for exponentiation);[b] dividing each exponent or scalar into a number of chunks or into a number of parts having a chunk or part width defined by a specific bit rate; and[c] individually recoding the chunks or parts (Notation paragraph 1, c is a recoded section of bits for the vector of exponent to be performed).

As per claim 2, Moller discloses a method as claimed in claim 1, characterized in that the exponent or scalar) is represented in the divided form E.sub.i = .SIGMA..sub.k=0.sup.r e.sub.i,k2.sup.kL, wherein r is defined as the number of chunks or parts, in particular as an integer quotient of the maximum bit rate and the bit rate of the chunk or part width, and 0 <= e.sub.i,k < 2.sup.L (A Framework for Exponentiation

[Page 2], paragraph 1, each exponent is broken into subsections of l bits where each exponent is less than the maximum bit length l).

As per claim 3, Moller discloses a method as claimed in claim 1, characterized in that the chunk or part width is selected to be significantly greater than a parameter which corresponds to the width, in particular to the upper limit of the width, of a window over which the bits of the respective exponent or scalar are read, and significantly shorter than the maximum length of each exponent or scalar , in particular is selected prior to method step [a.1] and/or [a.2] (Section 4 [Page 5], Paragraph 1-3, a window parameter w is the window size for every given exponent to be scanned).

As per claim 4, Moller discloses a method as claimed in claim 1, characterized in that in the case of exponentiation, method step [c] of recoding the chunks or parts can be divided into the following sub steps for each individual chunk or for each individual part of each exponent: [c. l] setting a temporary variable to a standardized value, in particular to the value 1 of the element of the group which is neutral with respect to the group operation assigned to the group (Section 3, A is set to 1_G); [c.2] successively setting a variable to the values r-1, r-2, 0, wherein for each value k=r-1, r-2, 0 of the variable the following sub steps are carried out (Section 3, for i=l down to zero): [c.2.i] for each value i=1, 2, d of an index, wherein d is defined as the number of elements, in particular depending on the number of exponents assigned to the elements (Section 3, for each element in the exponent $b_{j,i}$): [c.2.i.a] recoding the chunk or part as the sum of

powers of two weighted by in each case at least one coefficient deriving from at least one finite set of integers (Section 3, recoding the element to g^{bi2i}); [c.2.i.b] if the coefficient assigned to the highest power of two does not vanish: setting the temporary variable to the product of temporary variable and the power of the element which is assigned to the coefficient of the highest power of two; [c.2.ii] for each value j=L-1, L-2, 0 of the index (Section 3, if B is not zero selectively replacing A with new element): [c.2.ii.a] squaring the temporary variable (Section 3, $A = A^2$); [c.2.ii.b] for each value i=1, 2, d of the index: if the coefficient assigned to the power of two does not vanish: setting the temporary variable to the product of temporary variable and the power of the element which is assigned to the respective coefficient of the power of two; and after method step [c] of individually recoding the chunks or parts the temporary variable is returned (Section 3, if B is not zero perform operation on A and return A when final iteration complete).

As per claim 5, it is the method of claim 45. A method as claimed in claim 1, characterized in that in the case of scalar multiplication (Inherent [Section 1 [Page 1], line 20], applying the same windowing function to the scalar of a multiplication will result in the same steps as applying the window function to an exponent of an exponentiation), method step [c] of recoding the chunks or parts can be divided into the following sub steps for each individual chunk or for each individual part of each exponent: [c. l] setting a temporary variable to a standardized value, in particular to the value 1 of the element of the group which is neutral with respect to the group operation

assigned to the group (Section 3, A is set to 1_G); [c.2] successively setting a variable to the values r-1, r-2, 0, wherein for each value k=r-1, r-2, 0 of the variable the following sub steps are carried out (Section 3, for i=l down to zero): [c.2.i] for each value i=1, 2, d of an index, wherein d is defined as the number of elements, in particular depending on the number of exponents assigned to the elements (Section 3, for each element in the exponent $b_{j,i}$): [c.2.i.a] recoding the chunk or part as the sum of powers of two weighted by in each case at least one coefficient deriving from at least one finite set of integers (Section 3, recoding the element to g^{bi2i}); [c.2.i.b] if the coefficient assigned to the highest power of two does not vanish: setting the temporary variable to the product of temporary variable and the power of the element which is assigned to the coefficient of the highest power of two; [c.2.ii] for each value j=L-1, L-2, 0 of the index (Section 3, if B is not zero selectively replacing A with new element): [c.2.ii.a] squaring the temporary variable (Section 3, $A = A^2$); [c.2.ii.b] for each value i=1, 2, d of the index: if the coefficient assigned to the power of two does not vanish: setting the temporary variable to the product of temporary variable and the power of the element which is assigned to the respective coefficient of the power of two; and after method step [c] of individually recoding the chunks or parts the temporary variable is returned (Section 3, if B is not zero perform operation on A and return A when final iteration complete).

As per claim 6, Moller discloses a method as claimed in claim 1, characterized in that the recoded chunk or the recoded part is used once and the memory unit in which the recoded chunk or the recoded part is stored is used to recode the following chunk or the

following part (Section 3 [Page 5], lines 4 [equation for power product], for successive j in range 0 to k, e_j is reused).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 7-10 rejected under 35 U.S.C. 103(a) as being unpatentable over Moller in view of Tenca et al. (US 7,046,800) (hereinafter Tenca).

As per claim 7, Moller fails to disclose expressly, a method as claimed in claim 1, characterized in that the method is implemented on at least one microprocessor assigned in particular to at least one chip card and/or in particular to at least one smart card.

Tenca discloses a method as claimed in claim 1, characterized in that the method is implemented on at least one microprocessor assigned in particular to at least one chip card and/or in particular to at least one smart card (Column 15 lines 22-39, exponentiation can be performed in hardware modules as a microprocessor in a smart card).

Moller and Tenca are from the same field of endeavor as multiple exponentiation.

It would have been obvious at the time of the invention to modify the equations of Moller and implement them in a microprocessor on a smart card as shown in Tenca because it would allow for the advanced technique of applying multiple exponentiations to be used in a cryptographic system.

As per claim 8, Moller fails to disclose a microprocessor which operates in accordance with a method as claimed in claim 1.

Tenca discloses a microprocessor which operates in accordance with a method as claimed in claim 1 (Column 15 lines 22-39, exponentiation can be performed in hardware modules as a microprocessor in a smart card).

Moller and Tenca are from the same field of endeavor as multiple exponentiation.

It would have been obvious at the time of the invention to modify the equations of Moller and implement them in a microprocessor on a smart card as shown in Tenca because it would allow for the advanced technique of applying multiple exponentiations to be used in a cryptographic system.

As per claim 9, Moller fails to disclose expressly a device, in particular a chip card and/or in particular a smart card, having at least one microprocessor as claimed in claim 8.

Tenca discloses a device, in particular a chip card and/or in particular a smart card, having at least one microprocessor as claimed in claim 8 (Column 15 lines 22-39,

exponentiation can be performed in hardware modules as a microprocessor in a smart card).

Moller and Tenca are from the same field of endeavor as multiple exponentiation.

It would have been obvious at the time of the invention to modify the equations of Moller and implement them in a microprocessor on a smart card as shown in Tenca because it would allow for the advanced technique of applying multiple exponentiations to be used in a cryptographic system.

As per claim 10, Moller fails to disclose expressly the use of a method as claimed in claim 1 and/or of at least one microprocessor as claimed in claim 8 and/or of at least one device, in particular of at least one chip card and/or in particular of at least one smart card, as claimed in claim 9, in at least one cryptosystem, in particular in at least one public key cryptosystem, in at least one key exchange system or in at least one signature system.

Tenca discloses the use of a method as claimed in claim 1 and/or of at least one microprocessor as claimed in claim 8 and/or of at least one device, in particular of at least one chip card and/or in particular of at least one smart card, as claimed in claim 9, in at least one cryptosystem, in particular in at least one public key cryptosystem, in at least one key exchange system or in at least one signature system (Column 15 lines 22-39, exponentiation can be performed in hardware modules as a microprocessor in a smart card).

Moller and Tenca are from the same field of endeavor as multiple exponentiation.

It would have been obvious at the time of the invention to modify the equations of Moller and implement them in a microprocessor on a smart card as shown in Tenca because it would allow for the advanced technique of applying multiple exponentiations to be used in a cryptographic system.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KEVIN HUGHES whose telephone number is (571)270-3365. The examiner can normally be reached on M-Th/F 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lewis Bullock can be reached on 5712723759. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

December 18, 2010 /KEVIN HUGHES/

Examiner, Art Unit 2193

/Lewis A. Bullock, Jr./
Supervisory Patent Examiner, Art Unit 2193